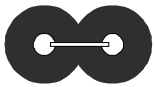
X.509 PDAM (September 1998) Issues:

Santosh Chokhani

chokhani@cygnacom.com

Issues (1/5)

- **Issue 1: Name and scope change to Public Key and Privilege Management**
- **Proposed US Position: Agree**
- **Issue 2: (a) Certificate appearing in at least one base CRL. (b) Information in base CRL if a certificate held and released**
- **Proposed US Position: (a) Must appear in a base CRL. (b) Need not appear in base CRL**

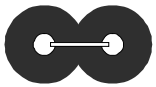


Issues (2/5)

- **Issue 3: Roles solely through attribute certificates**
- **Proposed US Position: Disagree**
- **Issue 4: Standard syntax for Access Control Policy**
- **Proposed US Position: Disagree.**
- **Rationale: The module has not been validated for accommodating various rule and role based policies. The policies generally are diverse, but simple. Having a single policy syntax makes for a very complex software implementation which may not be as well validated or tested, resulting in security flaws in critical access control decision function.**

Issues (3/5)

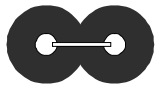
- **Issue 5: Out of Band Delegation**
- **Proposed US Position: Disagree. There too many unknown here in terms of how the delegation and delegation path will be verified.**
- **Issue 6: Matching on Attribute Certificates**
- **Proposed US Position: Add the following fields for matching and use matching rules akin to X.509 public key certificate matching rules (attrCertValidityPeriod; authorityAttributeIdentifier; ownerAttributeIdentifier)**



CYGNACOM SOLUTIONS

Issues (4/5)

- **Issue 7: CRL Processing Text Normative or Informative**
- **Proposed US Position: Most of the text proposed is Normative, specifically section M.3.4.1 through M.3.4.4 and their associated subsections**
- **Issue 8: Check for reason codes asserted in critical CRL DP(s)**
- **Proposed US Position: This is a change in the standard, but a good idea. Applications should be required to check for reason code(s) asserted in critical DP(s). If a critical DP has no reason code asserted, the application should be required to get a CRL that covers all reasons.**



Issues (5/5)

- **Issue 9: Distribution Point for Delta CRL Only**
- **Proposed US Position: No. security reasons, false sense of security, delta needs to correspond to a specific base**
- **Issue 10: Only Issue Indirect Delta CRL**
- **Proposed US Position: No. Any form of delta requires issuance of base. Delta needs to correspond to a specific base. It is ok to issue both base and delta as indirect. The requirement is for the issuer of both to be the same and not certificate issuer.**